ATM'LERİN GELİŞTİRİLMİŞ GÜVENLİK ÖZELLİĞİ

YÜZ TANIMA YOLUYLA

Bayan SOUNDARI D V
ECE Bölümü
Sri Krishna Mühendislik ve Teknoloji Koleji
Coimbatore, Hindistan
soundaridv@skcet.ac.in

ARAVINDH R
ECE Bölümü
Sri Krishna Mühendislik ve Teknoloji Koleji
Coimbatore, Hindistan
aravindh10100@gmail.com

EDWIN RAJ K
ECE Bölümü
Sri Krishna Mühendislik ve Teknoloji Koleji
Coimbatore, Hindistan
mathaenggvdsr@gmail.com

ABISHEK S
ECE Bölümü
Sri Krishna Mühendislik ve Teknoloji Koleji
Coimbatore, Hindistan
abishek.srinivasan@gmail.com

2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS) | 978-1-6654-1272-8/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICCS51141.2021.9432327

Özet- **ATM olarak da bilinen Otomatik Vezne Makineleri günümüzde herkes tarafından yaygın olarak kullanılmaktadır. ATM makinesi (Otomatik Vezne Makinesi), bankalar tarafından para çekme, para transferi gibi bankacılık işlemlerini gerçekleştirmek ve bir bankayı ziyaret etmeye gerek kalmadan bir kullanıcının banka hesabı hakkında birçok bilgi almak için kullanılan elektronik bir cihazdır. Bu Sistem, işlem yapma biçiminde devrim yarattı. Basit bir para çekme işlemi için banka önünde uzun kuyruklar oluşmuyordu. Bir bankanın sahip olduğu ATM sayısı, bankanın gücünü değerlendirmede bir faktör olabilir. ATM sayısındaki artışla birlikte ATM'lerdeki dolandırıcılık faaliyetlerinde de artış görülmektedir. Bu projenin ana motivasyonu ATM kullanımının güvenlik özelliğini arttırmaktır. Mevcut yöntem güvenlik için statik anahtar (PIN) kullanmaktadır. Önerilen yöntem, mevcut yöntemle birleştirilmiş bir anahtar olarak Face-id kullanmaktadır. Avantajları, yüz kimliğinin herkes için benzersiz olması ve kullanıcı dışında hiç kimse tarafından kullanılamamasıdır. Yüz kimliği taramasının uygulanması için makine öğrenimi ve görüntü işleme algoritmaları (Eigenface algoritması) kullanılmaktadır.**

Anahtar Kelimeler-ATM, Face-id, Eigenface algoritması, Makine Öğrenmesi.

I. GİRİŞ

Günümüzde ATM'lerin kullanımı günlük hayatımızın kaçınılmaz bir parçası haline gelmiştir. ATM'nin kullanılmaya başlanmasından önce insanlar ellerinde nakit para ile seyahat ederlerdi. Bu durum soyulma riskini doğuruyor ya da kullanıcının ihmali nedeniyle nakit para kaybolabiliyordu. Bu sorunların üstesinden gelmek için ATM büyük bir rol oynadı. Bir kartın içindeki nakit para gibidir. ATM teknolojisi geliştikçe, yanlış kullanım fikri de gelişti. Bu sistemin en büyük dezavantajı, eğer PIN kodu biliniyorsa, herhangi bir kişinin bunu para çekmek için kullanabilmesidir.

Bu sorunu çözmek için anahtar olarak Face-id kullanılır. Biyometrinin ana kullanımı, bir kişi için benzersiz olmasıdır. Önerilen yenilik, geleneksel ATM güvenlik sistemi için bir alternatif değildir. Önerilen yenilik, mevcut yöntem için ek bir destek olarak düşünülmektedir. Hindistan'da her yıl yaklaşık 2000 ATM suçu meydana gelmektedir. Önerilen yöntemin bu oranı büyük ölçüde azaltacağı kesindir.

II. İLGİLİ ÇALIŞMALAR

Mohsin Karovaliya makalesinde [2] yüz tanıma için Eigenface tabanlı bir yöntem önermektedir. Bu sistem önceki sistemlerde kullanılan algoritmaları analiz etmektedir. PCA tabanlı algoritma daha güvenilir, çok hızlı ve depolama alanı çok daha azdır. Bu yöntemin ana dezavantajı, kullanıcıların fotoğrafları kullanılarak manipüle edilebilmesidir. Bu yöntem 3D yüz maskeleri kullanılarak geliştirilebilir ancak 3D maskelerin yapım maliyeti çok yüksektir.

Makalede [3], soygun gerçekleştiğinde ATM makinesinden üretilen titreşimleri algılayan bir titreşim sensörü önerilmektedir. Bu sistem, ARM denetleyici tabanlı gömülü bir sistem kullanarak titreşim sensörü tarafından toplanan gerçek zamanlı verileri işler. Titreşim algılandığında buzzer bir bip sesi çıkaracaktır. ATM kapısı bir DC motor ile kapatılır. Ayrıca bazı ek güvenlik önlemleri de mevcuttur. Bu, hırsızlığı caydıracak ve şüphelinin tutuklanmasını mümkün kılacaktır. Yazılımı çalıştırmak için iki yazılım programı kullanılır, bunlardan ilki Keil Vision 3.0'dır. Flash sihirli simülatörü ise ikincisidir. Keil Vision Debugger, çip üzerindeki çevre birimlerini doğru şekilde simüle eder. Bu cihaz, ATM makinesinin çalındığını GSM teknolojisi ile gerçek zamanlı olarak tespit ederek hızlı tepki verilmesine ve arızanın en aza indirilmesine yardımcı olur.

Makalede [4], parmak izi tanıma, karşılık gelen iki parmak kodu arasındaki Öklid uzaklığı bulunarak curvelet dönüşümü ile yapılır. Test parmak kodu, veritabanındaki tüm parmak kodları ile karşılaştırılır. Eşleşirse, eşleşen kayıtlı cep telefonu numarasına bir OTP gönderilecektir. Ön işleme için yerleşik MATLAB özelliği 'imread' kullanılır. Histogram eşitleme yaklaşımı, bir histogramdaki yoğunluk dağılımını marjinal olarak kaydırarak bir görüntünün küresel kontrastını iyileştirir. Bu, düşük kontrastlı alanların genel kontrastı etkilemeden daha fazla kontrast elde etmesine yardımcı olur. Bu, esasen en yaygın güç değerlerini yayan histogram eşitleme ile elde edilir. Curvelet dönüşümü ve FFT de fonksiyon çıkarımı için kullanılabilir.

Makalede [5] OTP üretmek için GSM modülü eklenerek ATM güvenliği artırılmıştır. GSM teknolojileriyle ilgili bir ağ sorunu olduğunda, bu sistem bir OTP üreten bir ATM'ye bağlanmak için Bluetooth kullanır kullanıcının cep telefonundan ilişki. Bir SMS servis sağlayıcısına özel bir abonelik gerekmediğinden, GSM modemler SMS'e başlamak için hızlı ve kolay bir yol olabilir. Bir GSM modem, gerekli kablo ve yazılıma sahip normal bir GSM telefonu da olabilir. Bir GSM modem, seri porta veya USB portuna bağlanmak için gerekli kablo ve yazılım sürücüsüne sahip normal bir GSM telefonu da olabilir.

III. ÖNERILEN YÖNTEM

Çoğu insan ATM'yi pek çok amaç için ve pek çok senaryoda kullanır. Burada en yaygın üç senaryo ele alınmakta ve çözümler bulunmaktadır.

- Kullanıcı ATM makinesini kendisi kullanıyormuş gibi.
- Kullanıcı, kullanıcının isteği olmadan para almak için birileri tarafından tehdit edilirse.
- Kullanıcının arkadaşı kullanıcının kartını kullanırsa.

Öncelikle, bir kullanıcı ATM'ye girdiğinde iki seçenek sunulur. Kullanıcının kendi kartıyla gelmesi (1 numara) ya da kullanıcının arkadaşının kartıyla gelmesi (2 numara).

A. Kullanıcı ATM'yi kendi başına kullanır

Bir kullanıcı kendi başına ATM makinesini kullandığında, önce kartın takılması gerekir. Şimdi bir kamera kullanıcının görüntüsünü yakalar. Şimdi, yakalanan görüntü veritabanında saklanan görüntü ile karşılaştırılır. Her iki görüntü de eşleşirse (karşılaştırma kısmını Eigenface algoritması yapar), kimliği başarıyla doğrulandı mesajı görüntülenir. Şimdi kullanıcının PIN kodunu girmesi gerekir. Girilen PIN doğruysa, daha fazla işlem yapılabilir.

B. Kullanıcı birileri tarafından tehdit ediliyor

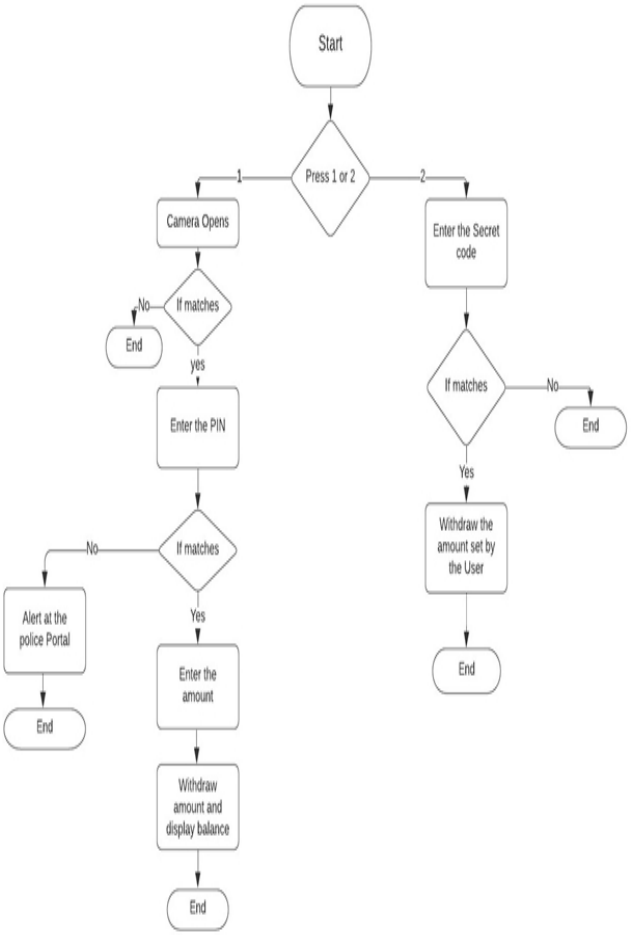
Şimdi kullanıcı para almak için birileri tarafından tehdit ediliyor. Bu senaryo için sağlam bir çözümümüz var. Önce kullanıcının yüzü eşleşecek. Şimdi doğru PIN'i girmek için kullanıcının yanlış bir PIN girmesi gerekir. Bu, arka uçta bulunan polis portalında bir uyarıya neden olur. İşlemler sorunsuzsa polis portalı atıl durumda olacaktır. Yanlış PIN girilirse uyarı alınır.

C. Kullanıcının arkadaşı kullanıcı kartı

Kullanıcının arkadaşı kartı kullandığında, yüzün eşleşmeyeceği açıktır. Bu durum için net bir yöntem önerdik. Kullanıcı mobil uygulamada bir PIN ve para çekme limiti belirlemelidir. Bu, her bir işlem için ayarlanmalıdır. Şimdi kullanıcının arkadaşı şunları yapmalıdır

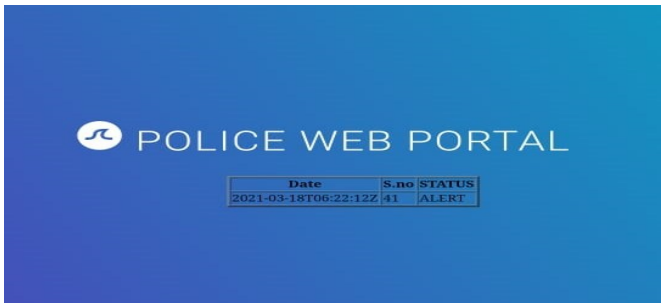
bu gizli PIN kodunu girin. PIN eşleşirse, kullanıcı tarafından belirlenen miktar otomatik olarak çekilecektir.

Akış Şeması




```
user@user-HP-Laptop-15-da1xxx:~/Desktop/ATM$ python3 Main.py
ENTER 1 FOR FACE TRANSACTION
 ENTER 2 FOR OTHER TRANSACTION1
0
SUCESSFULLY AUTHENTICATED
ENTER THE pin:1234
edwin
ENTER THE AMOUNT TO TAKE:100
AMOUNT PROCESSED SUCESSFULLY
Your Balance amount is
4900
ENTER 1 FOR FACE TRANSACTION
 ENTER 2 FOR OTHER TRANSACTION
```

csae1'in sonucu. Yüzün kimliği doğrulandı, PIN eşleşti. Şimdi miktar girilir. İşlem şu şekildedir başarıyla tamamlandı.



Vaka 2'nin sonucu: yüz eşleşirse ve PIN yanlış girilirse polise bir uyarı gönderilir arka uçtaki terminal.

```
user@user-HP-Laptop-15-da1xxx:~/Desktop/ATM$ python3 Main.py
ENTER 1 FOR FACE TRANSACTION
 ENTER 2 FOR OTHER TRANSACTION2
ENTER SECRET PIN:4567
-500
processed Sucessfully
ENTER 1 FOR FACE TRANSACTION
 ENTER 2 FOR OTHER TRANSACTION
```

Durum 3'ün sonucu: Kullanıcının arkadaşı kartı kullanırsa,

Ardından PIN (kullanıcı tarafından ayarlanan) doğru şekilde girilmelidir PIN miktarının doğru şekilde girilmesinden sonra geri çekildi.

MEVCUT SISTEMIN DEZAVANTAJLARI

- PIN kodunu bilen herkes kartı işlemler için kullanabilir.
- PIN statik olduğundan, suçluların bilgisayar korsanlığı yoluyla veya hatta kişiye uygulanan kaba kuvvet yoluyla kullanıcılardan çıkarması kolaydır.
- ATM kartlarındaki manyetik şeridin taranması kartın tüm ayrıntılarını verecektir. Bu da kartların çoğaltılmasına neden olur.
- ATM önünde insanları tehdit etmek bazı yerlerde yapılmaktadır ve PIN'in güvenlik özelliği bu durumlarda faydalı olamamaktadır.

ÖNERILEN SISTEMIN AVANTAJLARI

- Önerilen yöntem bir biyometrik kullanır, bu da mevcut sistemin güvenlik özelliğini büyük ölçüde artırır.
- Biyometrik kullandığımız için her birey için benzersizdir.
- Kullanıcıyı tehdit etme durumu burada iyi bir şekilde ele alınmıştır ve bu, kullanıcının ve kullanıcının parasının güvenliğiyle sonuçlanabilir.
- Kullanıcının arkadaşı kartı kullanırsa para çekme limiti belirlenir. Bu, kullanıcının hesabını kontrol etmesine yardımcı olur.
- Bu yöntemin uygulanması kolay, ucuz ve verimlidir.

Biyometri	Performans	Doğruluk	Maliyet
Iris	Orta	Orta	Yüksek
Parmak izi	Yüksek	Orta	Düşük
Retina	Yüksek	Yüksek	Yüksek

KULLANILAN ALGORITMALAR

Burada anahtar olarak yüz verilerini kullandığımız için. Burada görüntü işleme algoritmaları kullanıyoruz. Uygulama, görüntü tanıma algoritmalarında yerleşik olan python'da OpenCV kullanılarak yapılır. Algoritmalar makine öğrenimi kullanılarak eğitilir. Eigenface Algoritmasını kullanıyoruz.

YÜZ TANIMA

Yüz tanıma insanlar için kolay bir iştir. Yüzün geometrik özelliklerini görmek, yüz tanımada en kolay ve etkili yol olarak kabul edilir. İlk otomatik yüz tanımada kulakların konumu, burnun konumu gibi işaret noktaları kullanılmıştır. Bu noktalar, aralarındaki mesafe veya aralarındaki açı gibi özellik vektörünü çerçevelemede kullanıldı. Yüz tanıma işlemi, çekilen görüntünün özellik vektörü ile bir referans görüntü arasındaki mesafenin bulunmasıyla gerçekleştirilmiştir. Geometrik yüz tanıma üzerine yapılan son çalışmalardan bazıları, 22 boyutlu bir özellik vektörüydü ve büyük veri kümeleri üzerinde yapılan deneyler, geometrik özelliklerin tek başına yüz tanıma için yeterli bilgi taşımayabileceğini göstermiştir.

Temel olarak Bilgisayar kodlu yüz tanıma, insan beyninin yüzleri tanımak için kullandığı adımlarla aynı olan üç basit aşamaya ayrılabilir. Bu adımlar şunlardır:

(1) Veri Toplama: Tanımak istediğiniz kişilerin yüz verilerini (bu durumda yüz görüntülerini) toplayın.

(2) Tanıyıcıyı Eğitin: Tanıyıcıya yüz verilerinin yanı sıra hatırlayabilmesi için her bir yüzün adını da verin.

(3) Tanıma: Yüz tanıyıcıyı, onları nasıl tanıdığını görmek için belirli kişilerin yeni yüzleriyle besleyin.

OpenCV'nin iki yerleşik yüz tanıyıcısı vardır. Bu yüz tanıyıcıların isimleri şunlardır: Eigenfaces ve Fisher faces.

3.3.4 Özyüzler Yüz Tanıma Algoritması

Bu algoritmada, bir yüz görüntüsü yüksek boyutlu bir görüntü uzayından bir noktadır ve sınıflandırmanın kolaylaştığı daha düşük boyutlu bir temsil bulunur. Düşük boyutlu alt uzay, maksimum varyansa sahip eksenleri tanımlayan Temel Bileşen Analizi (PCA) ile bulunur. Bu tür bir dönüşüm yeniden yapılandırma açısından optimal olsa da, herhangi bir sınıf etiketini dikkate almaz. Varyansın dış kaynaklardan üretildiği bir durum düşünün, bu ışık olsun. Maksimum varyansa sahip eksenlerin herhangi bir ayırt edici bilgi içermesi gerekmez, dolayısıyla bir sınıflandırma imkansız hale gelir.

Algoritmanın işleyişi, bir yüzü tanımak için yüzün tüm bölümlerinin eşit derecede önemli olmadığını göz önünde bulundurmasıdır. Bunun yerine, burun şekli, kulaklar, alın gibi ana özellikler kullanılır ve bunların birbirlerinden ne kadar farklı oldukları göz önünde bulundurulur Ana fikir, maksimum farklılığa sahip bölgeyi bulmaktır. Gözler ve burun bölgesini karşılaştırdığımızda ciddi miktarda varyasyon olacağını düşünelim. Birden fazla yüz karşılaştırılacağı zaman, yüzler arasındaki karşılaştırma, yüzler arasındaki maksimum varyasyona bakılarak yapılır ve yüzlerin ayırt edilmesine yardımcı olur. Eigenfaces tanıyıcının arkasındaki süreç budur. Bu tanıyıcı, eğitmek için kullanılan tüm resimlere bakarak çalışır ve ilgili olduğu düşünülen temel bileşenleri çıkarır ve diğer bileşenleri göz ardı eder. Bu anahtar bileşenler Ana bileşenler olarak adlandırılır ve bunlar tanıyıcı için ana kaynak olarak işlev görür.

Bu yüz tanıyıcı aynı zamanda yüzün kayıtlarını kaydı olan kişiyle eşleştirir. Dolayısıyla, yeni bir kayıt eklenmesi gerektiğinde aşağıdaki süreç izlenir. Önce temel bileşen çıkarılır. Daha sonra eğitmek için kullanılan görüntülerle karşılaştırma işlemi yapılır. En iyi eşleşen görüntü bulunur. Şimdi kaydı kişi adı ile eşleştirin. Özyüz tanıyıcıda ışık önemli ihtiyaçlardan biri olarak hareket eder. Sadece ışık yardımı ile yüzün gölgeli ve ışıklı kısımları bulunur. Bu ayrıntılar, bir yüzü temsil etmek için kullanılan bir özyüz bulmak için kullanılır. İki gözün, bir burnun, bir ağzın gölgeleri ve şekilleri yüz tanımada en çok kullanılan parametredir.

Eigenface algoritmasının nasıl çalıştığını gösteren resim.

IV. SONUÇ

Özetle, önerdiğimiz yöntem güvenlik özelliğini artırmada çok daha iyidir. Çalışmamızın temel amacı, kullanıcının daha iyi olması için mevcut geleneksel yöntemle birlikte yüz tanıma özelliğini dahil etmektir. Burada kullanılan Eigenface algoritması, kullanıcının yüzünü veritabanındaki yüz ile karşılaştırmak için kullanılır. Makine öğrenimi, yüz tanıyıcıyı eğitmek için kullanılır (OpenCV dahili yüz tanıyıcıda kullanılır). Adaboost yüz tanıma algoritması %75 başarı oranına sahiptir ancak eigenface Algoritması %80 başarı oranı üretir.

Bu sistemin ana sınırlaması, kameraların periyodik bakımını gerektirmesidir. İkizler bu sistemde bir istisna olabilir. Nadir durumlarda, fotoğraflar güvenliği atlatmak için kullanılabilir. Bu yöntemin gelecekteki kapsamı, yüksek kaliteli dayanıklı kameraların kullanılmasıdır. İkizlerin durumu ve fotoğraf atlama için 3 boyutlu kameralar kullanılabilir.

REFERANSLAR

[1] J.J.Patoliya, M.M. Desai, "Gömülü Linux Platformu kullanan Yüz Algılama tabanlı ATM Güvenlik Sistemi", *2nd International Conference for Convergence in Technology (I2CT),* 2017.

[2] M.Karovaliyaa, S.Karediab, S.Ozac, Dr.D.R.Kalbande, "Enhanced security for ATM machine with OTP and Facial recognition features",*International Conference on Advanced Computing Technologies and Applications (ICACTA),* 2015.

[3] [3]Sivakumar T. 1 , G. Askok 2 , k. S. Venuprathap, "Design and Implementation of Security Based ATM theft Monitoring system", *International Journal of Engineering Inventions,* Volume 3, Issue 1, 2013.

[4] [4]C. Bhosale, P. Dere, C. Jadhav, "ATM security using face and fingerprint recognition", *Interna- tional Journal of Research in Engineering, Technology and Science,* Volume VII, Special Issue, Feb 2017.

[5] [5]Manoj V , M. Sankar R , Sasipriya S , U. Devi E, Devika T , "Multi Authentication ATM Theft Prevention Using iBeacon", *International Research Journal of Engineering and Technology (IRJET).*

[6] L. Wang,H. Ji, Y. Shi, "Face recognition using maximum local fisher discriminant analysis",18th IEEE International Conference on Image Processing, 2011

[7] K.Shailaja and Dr.B.Anuradha, "Effective Face Recognition using Deep Learning based Linear Discriminant Classification", *IEEE International conference on Computational Interlligence and Computing Research,2016.*

[8] H. R. Babaei, O. Molalapata and A.H.Y Akbar Pandor, "Face Recognition Application for Au- tomatic Teller Machines (ATM)",International Conference on Information and Knowledge Management(ICIKM),2012.

[9] Chen, Joy Iong Zong. "Uçucu Alanlarda Şüpheli Faaliyet Tespiti için Akıllı Güvenlik Sistemi." Bilgi Teknolojileri Dergisi 2, no. 01 (2020): 64-72.

[10] Suma, V. "İnsan-makine etkileşimi için bilgisayar görüşü-inceleme." Journal of trends inComputer Science and Smart technology (TCSST) 1, no. 02 (2019): 131-139.

[11] Rika Rosnelly, Mutiara S. Simanjuntak, Ade Clinton sitepu, Mulkan Azhari, Sandy Kosasi tarafından 2020'de Dizüstü bilgisayar kamerasında Eigenface algoritması kullanılarak Yüz Tanıma 8th Uluslararası Siber ve BT hizmet Yönetimi Konferansı.

[12] Delpiah Wahyuningsih, Chanda Kirana, Rahmat Sulaiman, Hamidah, Triwanto tarafından 2019 7th Uluslararası Siber ve BT Hizmet Yönetimi Konferansı'nda (CITSM) yüz tanıma sürecinde Eigen yüz ve Fisher Yüz Algoritmasının performansının karşılaştırılması.

[13] Gömülü Linux platformu kullanan Yüz Algılama tabanlı ATM güvenlik sistemi Jignesh J. Patoliya, Miral M Desai 2017 2nd International Conference for Convergence in Technology(I2CT).

[14] Eigenfaces, LBPH ve Fisher Algorithms kullanarak Gerçek Zamanlı Yüz İfadesi ve duygu tanıma Shrayan Mukhopadhyay, Shilpu Sharma 2020 10th International Conference on cloud computing, Data Science and Engineering.

[15] Yüz tanıma uyarı mekanizması ve Web Hizmetleri ile kullanıcı hareketini izlemek için ideallik C. Jayaprakash, V Maheshwari 2016 10th International Conference on Intelligent Systems and Control(ISCO).